

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-339153

(43)Date of publication of application : 08.12.2000

(51)Int.Cl.

G06F 9/06

(21)Application number : 11-145517

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>

(22)Date of filing : 25.05.1999

(72)Inventor : SUZUKI KATSUHIKO

NIWANO EIICHI

CHIBA NOBUHIRO

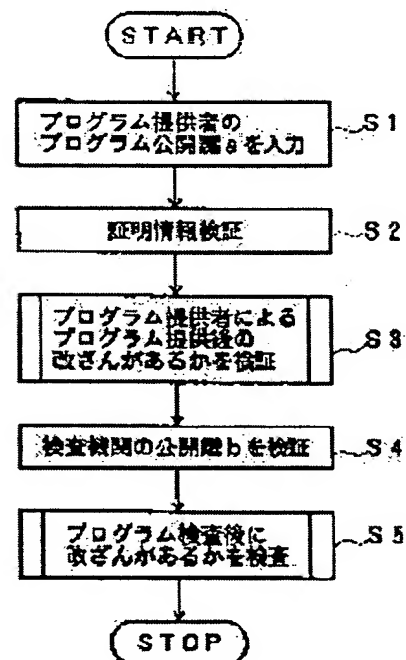
HOSODA YASUHIRO

(54) METHOD AND DEVICE FOR VERIFYING PROGRAM AND STORAGE MEDIUM STORING PROGRAM VERIFICATION PROGRAM

(57)Abstract:

PROBLEM TO BE SOLVED: To verify that a supplied program safely operates by permitting an inspection organization to decide whether the program executed after the inspection of the operation of the program is falsified or not.

SOLUTION: When an open key (c) for verifying information is given (S1), proof information (a) is verified by the open key (c), and the open key (a) of a program supplier is recognized (S2). Information obtained by decoding ciphering information (a) by the open key (a) and a password algorithm corresponding to the identifier (a) of the password algorithm is compared with the hash value of a program in order to decide whether the program is falsified or not after it has been supplied (S3). Proof information (b) is verified by the open key (c), and the open key (b) of an inspection organization inspecting the operation of the program is recognized (S4). Information obtained by decoding ciphering information (b) by the open key (b) and the password algorithm corresponding to identification information (b) of the password algorithm is compared with the hash value of the program in order to decide whether the program is falsified or not after the operation has been inspected (S5).



LEGAL STATUS

[Date of request for examination]

13.08.2002

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the
examiner's decision of rejection or application
converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of
rejection]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-339153

(P2000-339153A)

(43) 公開日 平成12年12月8日 (2000.12.8)

(51) Int.Cl.⁷

G 0 6 F 9/06

識別記号

5 5 0

F I

G 0 6 F 9/06

テ-マ-ト* (参考)

5 5 0 E 5 B 0 7 6

5 5 0 Z

審査請求 未請求 請求項の数 3 O L (全 8 頁)

(21) 出願番号

特願平11-145517

(22) 出願日

平成11年5月25日 (1999.5.25)

(71) 出願人 000004226

日本電信電話株式会社

東京都千代田区大手町二丁目3番1号

(72) 発明者 鈴木 勝彦

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(72) 発明者 庭野 栄一

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(74) 代理人 100070150

弁理士 伊東 忠彦

最終頁に続く

(54) 【発明の名称】 プログラム検証方法及び装置及びプログラム検証プログラムを格納した記憶媒体

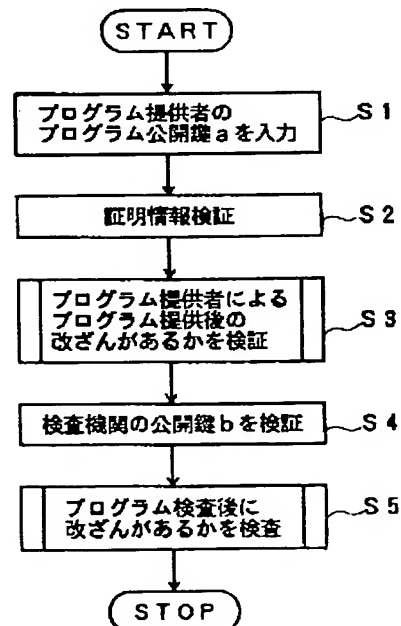
(57) 【要約】

(修正有)

【課題】 プログラム提供者のプログラム提供後、また検査機関のプログラム動作の検査後にプログラム改竄がないかの検証を行う。

【解決手段】 プログラムファイルと、証明機関の証明情報を検証するための公開鍵cが与えられると、公開鍵cにより証明情報aを検証し、公開鍵aがプログラム提供者の公開鍵であることを証明し、暗号化情報aを公開鍵aと暗号化アルゴリズムの識別子aに対応した暗号化アルゴリズムで復号した情報とプログラムのハッシュ値を比較し、プログラム提供者の提供後にプログラムの改竄が行われていないかの検出を行い、公開鍵cにより証明情報bを検証することにより、公開鍵bがプログラムの動作を検査した検査機関の公開鍵であることを証明し、暗号化情報bを公開鍵bと暗号化アルゴリズムの識別情報bに対応した暗号化アルゴリズムで復号した情報とプログラムのハッシュ値を比較し、プログラムの動作を検査した後に、該プログラムの改竄が行われていないかの検出を行う。

本発明の原理を説明するための図



【特許請求の範囲】

【請求項1】 コンピュータの制御を記述したプログラムを検証するプログラム検証方法において、検証の対象のプログラムと、該プログラムのハッシュ値をプログラム提供者のみが知る提供者秘密鍵aで暗号化した暗号化情報aと、該暗号化情報aを生成するために利用したハッシュアルゴリズムと暗号アルゴリズムの識別情報aと、該暗号化情報aを復号するための公開鍵aと証明機関が発行した公開鍵aに対するお墨付きを示す証明情報aと、プログラムのハッシュ値をプログラムの動作を検査した検査機関のみが知る検査機関秘密鍵bで暗号化した暗号化情報bと、該暗号化情報bを生成するために利用したハッシュアルゴリズムと暗号アルゴリズムの識別情報bと、該暗号化情報bを復号するための公開鍵bと該証明機関が発行した公開鍵bに対するお墨付きを示す証明情報bからなるプログラムファイルと、証明機関のお墨付きを示す情報を検証するための公開鍵cが与えられると、前記公開鍵cにより前記証明情報aを検証し、前記公開鍵aが前記プログラム提供者の公開鍵であることを証明し、前記暗号化情報aを前記公開鍵aと暗号アルゴリズムの識別子aに対応した暗号アルゴリズムで復号した情報とプログラムのハッシュ値を比較し、前記プログラム提供者がプログラムを提供した後にプログラムの改竄が行われていないかの検出を行い、前記公開鍵cにより前記証明情報bを検証することにより、前記公開鍵bがプログラムの動作を検査した検査機関の公開鍵であることを証明し、前記暗号化情報bを前記公開鍵bと暗号アルゴリズムの識別情報bに対応した暗号アルゴリズムで復号した情報とプログラムのハッシュ値を比較し、前記プログラムの動作を検査した後に、該プログラムの改竄が行われていないかの検出を行うことを特徴とするプログラム検索方法。

【請求項2】 コンピュータの制御を記述したプログラムを検証するプログラム検証方法において、検証の対象のプログラムと、該プログラムのハッシュ値をプログラム提供者のみが知る提供者秘密鍵aで暗号化した暗号化情報aと、該暗号化情報aを生成するために利用したハッシュアルゴリズムと暗号アルゴリズムの識別情報aと、該暗号化情報aを復号するための公開鍵aと証明機関が発行した公開鍵aに対するお墨付きを示す証明情報aと、プログラムのハッシュ値をプログラムの動作を検査した検査機関のみが知る検査機関秘密鍵bで暗号化した暗号化情報bと、該暗号化情報bを生成するために利用したハッシュアルゴリズムと暗号アルゴリズムの識別情報bと、該暗号化情報bを復号するための公開鍵bと該証明機関が発行した公開鍵bに対するお墨付きを示す証明情報bからなるプログラムファイルと、

前記プログラムファイルと、証明機関のお墨付きを示す情報を検証するための公開鍵cを入力する入力手段と、前記公開鍵cにより前記証明情報aを検証する手段と、前記公開鍵aが前記プログラム提供者の公開鍵であることを証明する手段と、前記暗号化情報aを前記公開鍵aと暗号アルゴリズムの識別子aに対応した暗号アルゴリズムで復号した情報とプログラムのハッシュ値を比較する手段と、前記プログラム提供者がプログラムを提供した後にプログラムの改竄が行われていないかの検出を行う手段とを有するプログラム提供者検証手段と、前記公開鍵cにより前記証明情報bを検証することにより、前記公開鍵bがプログラムの動作を検査した検査機関の公開鍵であることを証明する手段と、前記暗号化情報bを該公開鍵bと暗号アルゴリズムの識別情報bに対応した暗号アルゴリズムで復号した情報とプログラムのハッシュ値を比較する手段と、前記プログラムの動作を検査した後に、該プログラムの改竄が行われていないかの検出を行う手段とを有する検査機関検証手段とを有することを特徴とするプログラム検索装置。

【請求項3】 コンピュータの制御を記述したプログラムを検証するプログラム検証プログラムを格納した記憶媒体であって、

検証の対象のプログラムと、該プログラムのハッシュ値をプログラム提供者のみが知る提供者秘密鍵aで暗号化した暗号化情報aと、該暗号化情報aを生成するために利用したハッシュアルゴリズムと暗号アルゴリズムの識別情報aと、該暗号化情報aを復号するための公開鍵aと証明機関が発行した公開鍵aに対するお墨付きを示す証明情報aと、プログラムのハッシュ値をプログラムの動作を検査した検査機関のみが知る検査機関秘密鍵bで暗号化した暗号化情報bと、該暗号化情報bを生成するために利用したハッシュアルゴリズムと暗号アルゴリズムの識別情報bと、該暗号化情報bを復号するための公開鍵bと該証明機関が発行した公開鍵bに対するお墨付きを示す証明情報bからなるプログラムファイルと、証明機関のお墨付きを示す情報を検証するための公開鍵cを入力させる入力プロセスと、

前記公開鍵cにより前記証明情報aを検証するプロセスと、前記公開鍵aが前記プログラム提供者の公開鍵であることを証明するプロセスと、前記暗号化情報aを前記公開鍵aと暗号アルゴリズムの識別子aに対応した暗号アルゴリズムで復号した情報とプログラムのハッシュ値を比較するプロセスと、前記プログラム提供者がプログラムを提供した後にプログラムの改竄が行われていないかの検出を行うプロセスとを有するプログラム提供者検証プロセスと、

前記公開鍵cにより前記証明情報bを検証することにより、前記公開鍵bがプログラムの動作を検査した検査機関の公開鍵であることを証明するプロセスと、前記暗号化情報bを該公開鍵bと暗号アルゴリズムの識別情報b

に対応した暗号アルゴリズムで復号した情報とプログラムのハッシュ値を比較するプロセスと、前記プログラムの動作を検査した後に、該プログラムの改竄が行われていないかの検出を行うプロセスとを有する検査機関検証プロセスとを有することを特徴とするプログラム検索プログラムを格納した記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、プログラム検証方法及び装置及びプログラム検証プログラムを格納した記憶媒体に係り、特に、プログラム提供者がプログラムを提供した後に行われたプログラムの改竄の検出、検査機関がプログラムの動作を検査した後に行われたプログラムの改竄の検出を行うためのプログラム検証方法及び装置及びプログラム検証プログラムを格納した記憶媒体に関する。

【0002】

【従来の技術】従来、情報提供者が情報Aと当該情報Aのハッシュ値を当該情報Aの情報提供者のみが知る秘密鍵で暗号化した暗号化情報Bと、暗号化情報Bを復号するための公開鍵と証明機関の公開鍵に対するお墨付きを示す証明情報Cを組として配布し、その配布された情報(B+C)を受け取った利用者が、暗号化情報Bを公開鍵により復号した復号情報Dと元の情報Aのハッシュ値とを比較することで、情報提供者が情報Aを提供した後に情報の改竄が行われていないかを検証する方法がある。

【0003】

【発明が解決しようとする課題】しかしながら、上記従来の情報の配布方法でプログラムを配布した場合、プログラム提供者がプログラムを提供した後、プログラムが改竄されていないかの検証は可能であるが、プログラムを実行した場合、プログラムが不正な動作をするかの識別は不可能である。

【0004】本発明は、上記の点に鑑みなされたもので、プログラム提供者がプログラムを提供した後、プログラムが改竄されていないかの検証と、検査機関がプログラムの動作の検査をした後に行われたプログラムが改竄されていないかの検証を行うことにより、提供されたプログラムが安全に動作することを証明することが可能なプログラム検証方法及び装置及びプログラム検証プログラムを格納した記憶媒体を提供することを目的とする。

【0005】

【課題を解決するための手段】図1は、本発明の原理を説明するための図である。本発明（請求項1）は、コンピュータの制御を記述したプログラムを検証するプログラム検証方法において、検証の対象のプログラムと、該プログラムのハッシュ値をプログラム提供者のみが知る提供者秘密鍵aで暗号化した暗号化情報aと、該暗号化

情報aを生成するために利用したハッシュアルゴリズムと暗号アルゴリズムの識別情報aと、該暗号化情報aを復号するための公開鍵aと証明機関が発行した公開鍵aに対するお墨付きを示す証明情報aと、プログラムのハッシュ値をプログラムの動作を検査した検査機関のみが知る検査機関秘密鍵bで暗号化した暗号化情報bと、該暗号化情報bを生成するために利用したハッシュアルゴリズムと暗号アルゴリズムの識別情報bと、該暗号化情報bを復号するための公開鍵bと該証明機関が発行した公開鍵bに対するお墨付きを示す証明情報bからなるプログラムファイルと、証明機関のお墨付きを示す情報を検証するための公開鍵cが与えられると（ステップ1）、公開鍵cにより証明情報aを検証し、公開鍵aがプログラム提供者の公開鍵であることを証明し（ステップ2）、暗号化情報aを公開鍵aと暗号アルゴリズムの識別子aに対応した暗号アルゴリズムで復号した情報とプログラムのハッシュ値を比較し、プログラム提供者がプログラムを提供した後にプログラムの改竄が行われていないかの検出を行い（ステップ3）、公開鍵cにより証明情報bを検証することにより、公開鍵bがプログラムの動作を検査した検査機関の公開鍵であることを証明し（ステップ4）、暗号化情報bを公開鍵bと暗号アルゴリズムの識別情報bに対応した暗号アルゴリズムで復号した情報とプログラムのハッシュ値を比較し、プログラムの動作を検査した後に、該プログラムの改竄が行われていないかの検出を行う（ステップ5）。

【0006】図2は、本発明の原理構成図である。本発明（請求項2）は、コンピュータの制御を記述したプログラムを検証するプログラム検証方法において、検証の対象のプログラムと、該プログラムのハッシュ値をプログラム提供者のみが知る提供者秘密鍵aで暗号化した暗号化情報aと、該暗号化情報aを生成するために利用したハッシュアルゴリズムと暗号アルゴリズムの識別情報aと、該暗号化情報aを復号するための公開鍵aと証明機関が発行した公開鍵aに対するお墨付きを示す証明情報aと、プログラムのハッシュ値をプログラムの動作を検査した検査機関のみが知る検査機関秘密鍵bで暗号化した暗号化情報bと、該暗号化情報bを生成するために利用したハッシュアルゴリズムと暗号アルゴリズムの識別情報bと、該暗号化情報bを復号するための公開鍵bと該証明機関が発行した公開鍵bに対するお墨付きを示す証明情報bからなるプログラムファイル1と、プログラムファイル1と、証明機関のお墨付きを示す情報を検証するための公開鍵cを入力する入力手段2と、公開鍵cにより証明情報aを検証する手段と、公開鍵aがプログラム提供者の公開鍵であることを証明する手段と、暗号化情報aを公開鍵aと暗号アルゴリズムの識別子aに対応した暗号アルゴリズムで復号した情報とプログラムのハッシュ値を比較する手段と、プログラム提供者がプログラムを提供した後にプログラムの改竄が行われてい

ないかの検出を行う手段とを有するプログラム提供者検証手段3と、公開鍵cにより証明情報bを検証することにより、公開鍵bがプログラムの動作を検査した検査機関の公開鍵であることを証明する手段と、暗号化情報bを該公開鍵bと暗号アルゴリズムの識別情報bに対応した暗号アルゴリズムで復号した情報とプログラムのハッシュ値を比較する手段と、プログラムの動作を検査した後に、該プログラムの改竄が行われていないかの検出を行う手段とを有する検査機関検証手段4とを有する。

【0007】本発明（請求項3）は、コンピュータの制御を記述したプログラムを検証するプログラム検証プログラムを格納した記憶媒体であって、検証の対象のプログラムと、該プログラムのハッシュ値をプログラム提供者のみが知る提供者秘密鍵aで暗号化した暗号化情報aと、該暗号化情報aを生成するために利用したハッシュアルゴリズムと暗号アルゴリズムの識別情報aと、該暗号化情報aを復号するための公開鍵aと証明機関が発行した公開鍵aに対するお墨付きを示す証明情報aと、プログラムのハッシュ値をプログラムの動作を検査した検査機関のみが知る検査機関秘密鍵bで暗号化した暗号化情報bと、該暗号化情報bを生成するために利用したハッシュアルゴリズムと暗号アルゴリズムの識別情報bと、該暗号化情報bを復号するための公開鍵bと該証明機関が発行した公開鍵bに対するお墨付きを示す証明情報bからなるプログラムファイルと、証明機関のお墨付きを示す情報を検証するための公開鍵cを入力させる入力プロセスと、公開鍵cにより証明情報aを検証するプロセスと、公開鍵aがプログラム提供者の公開鍵であることを証明するプロセスと、暗号化情報aを公開鍵aと暗号アルゴリズムの識別子aに対応した暗号アルゴリズムで復号した情報とプログラムのハッシュ値を比較するプロセスと、プログラム提供者がプログラムを提供した後にプログラムの改竄が行われていないかの検出を行うプロセスとを有するプログラム提供者検証プロセスと、公開鍵cにより証明情報bを検証することにより、公開鍵bがプログラムの動作を検査した検査機関の公開鍵であることを証明するプロセスと、暗号化情報bを該公開鍵bと暗号アルゴリズムの識別情報bに対応した暗号アルゴリズムで復号した情報とプログラムのハッシュ値を比較するプロセスと、プログラムの動作を検査した後に、該プログラムの改竄が行われていないかの検出を行うプロセスとを有する検査機関検証プロセスとを有する。

【0008】上記のように、本発明によれば、プログラム提供者がプログラムを提供した後に行われたプログラムの改竄を検出するのみならず、検査機関がプログラムの動作を検査した後に行われた当該プログラムの改竄の双方を検出することが可能となる。

【0009】

【発明の実施の形態】図3は、本発明のシステム構成を

示す。同図に示すシステムは、ICチップ10、端末20及び証明機関サーバ30から構成され、端末20と証明機関サーバ30とがネットワークで接続されている。

【0010】以下では、本発明の動作を行うコンピュータをICチップとして説明する。図4は、本発明のICチップの構成を示す。ICチップ10は、端末20と通信を行うための入出力インタフェース13、情報を格納するためのメモリ11、メモリ11に格納された情報の演算を行うプロセッサ12からなり、1つのチップで構成される。

【0011】プロセッサ12は、ハッシュ生成部121、署名復号部122、及びデータ比較部123から構成される。ハッシュ生成部121は、MD5、SHA等の暗号アルゴリズム識別情報とプログラム等のデータを入力とし、当該データのハッシュを生成する。署名復号部122は、RSA、ESIGN等の暗号アルゴリズム識別情報と暗号化された暗号化データを入力とし、当該暗号アルゴリズム識別情報と暗号化データを復号する。

【0012】データ比較部123は、ハッシュ生成部121で生成されたハッシュ値と署名復号部122で復号された復号データとを比較する。図5は、本発明の端末の構成を示す。端末20は、ICチップ10の制御を行うためのプログラムファイルを格納するためのメモリ21とICチップ10と通信を行うための入出力インタフェース22とを有する。また、ネットワークにより証明機関サーバ30からの証明機関の公開鍵を取得する機能を有する。

【0013】メモリ21には、プログラムと、署名a、暗号アルゴリズム識別子a、証明書aの組と、署名b、暗号アルゴリズム識別子b、証明書bの2つの組が格納されている。秘密鍵aは、当該プログラムの提供者のみが知るRSA、ESIGN等の署名アルゴリズムの秘密鍵である。

【0014】署名aは、MD5等のハッシュアルゴリズムにより生成してプログラムのハッシュ値を入力とし、RSA、ESIGN等の署名アルゴリズムにより生成した署名である。暗号アルゴリズム識別子aは、署名aを生成するために利用した署名アルゴリズムとハッシュアルゴリズムを示す暗号アルゴリズム識別子である。

【0015】証明書aは、秘密鍵aと対である公開鍵aに対するお墨付き情報であるOSIのX.509に従った証明書である。署名bは、プログラムの動作を検査した検査機関のみが知るRSA、ESIGN等の署名アルゴリズムの秘密鍵bとMD5、SHA等のハッシュアルゴリズムにより生成したプログラムのハッシュ値を入力とし、RSA、ESIGN等の署名アルゴリズムにより生成した署名である。

【0016】暗号アルゴリズム識別子bは、署名bを生成するために利用した署名アルゴリズムとハッシュアルゴリズムを示す識別子である。証明書bは、秘密鍵bで

対である公開鍵bに対するお墨付き情報であるOSIのX.509勧告に従って作成された証明書である。端末20は、最初に、ネットワークにより接続された証明機関サーバ30から証明機関が発行する公開鍵を取得し、入出力インタフェース22によりICチップ10に転送する。

【0017】次に、端末20のメモリ21に格納されているプログラムファイル211を読み出し、入出力インタフェース22によりICチップ10に転送する。次に、ICチップ10の入出力インタフェース13において、端末20から転送された公開鍵及びプログラムファイルを取得して、メモリ11に格納する。これにより、図5に示されるプログラムファイル211の内容が当該メモリ11に格納されることになる。これにより、プロセッサ12では、当該メモリ11に格納されたプログラムファイルを読み込んで処理を行う。

【0018】本発明の検証の方法を以下に示す。図6は、本発明のプログラム提供後の改竄を検証する処理のフローチャートである。

ステップ101) ICチップ10のプロセッサ12は、メモリ11に格納されたプログラムファイルに含まれる証明書aをOS1のX-509勧告に従い検証する。

【0019】詳しくは、

① メモリ11に格納されたプログラムファイル中の証明書aに対する署名情報を除く証明書aの情報と証明書aに含まれる署名アルゴリズム情報を入力とし、ハッシュ生成部121により、対応する暗号アルゴリズムにより演算を実行し、ハッシュ値Aを生成する。

【0020】② 署名復号部122において、メモリ11に格納された証明機関の公開鍵と証明書aに対する署名情報と証明書aに含まれる署名アルゴリズム情報を入力とし、対応する暗号アルゴリズムにより演算を実行し、復号された復号情報Aを生成する。

③ データ比較部123は、生成したハッシュ値Aと復号された復号情報Aを入力とし、双方の比較を行い、一致すれば、証明機関が証明書aを発行した後に、証明書aが第三者により改竄されていないことが保証される。

【0021】ステップ102) 次に、証明書aの改竄が検出されない場合、署名aの検証を行う。

ステップ103) メモリ11に格納されたプログラムと署名aの生成に利用した暗号アルゴリズム識別子aを入力とし、ハッシュ生成部121により対応する暗号アルゴリズムにより演算を実行し、プログラムのハッシュ値Cを生成する。

【0022】ステップ104) メモリ11に格納された署名aと証明書aに含まれる公開鍵aと暗号アルゴリズム識別子を入力とし、署名復号部122で対応する暗号アルゴリズムにより演算を実行し、復号された復号情報Cを生成する。

ステップ105) 次にデータ比較部123において、ハッシュ生成部121で生成されたハッシュ値Cと復号情報Cを入力とし、データの比較を行う。

【0023】ステップ106) 比較した結果が一致すれば、プログラム提供者がプログラムを提供した後に、第三者によるプログラムが改竄されていないことが証明される。次に、上記の処理に引き続いて、検査機関のプログラム動作の検査後におけるプログラムの改竄を検証する動作を説明する。

【0024】図7は、本発明の検査機関のプログラム動作の検査後の改竄を検証する処理のフローチャートである。

ステップ201) プログラムの動作の検査機関の証明書bを公開鍵cにより検証することにより、公開鍵bがプログラムの動作を検査した検査機関の公開鍵であることを証明を検証する。検証方法は、前述の図6のフローチャートのステップ101と同様である。

【0025】ステップ202) 証明書bの改竄が検出されない場合には、証明書bは正規のものとする。

ステップ203) 証明書bが正規である場合には、メモリ11に格納されたプログラムと署名bの生成に利用した暗号アルゴリズム識別子bを入力とし、ハッシュ生成部121により対応する暗号アルゴリズムにより演算を実行し、プログラムのハッシュ値Dを生成する。

【0026】ステップ204) メモリ11に格納された署名bと証明書bに含まれる公開鍵bと暗号アルゴリズム識別子を入力とし、署名復号部122で対応する暗号アルゴリズムにより演算を実行し、復号された復号情報Dを生成する。

ステップ205) 次にデータ比較部123において、ハッシュ生成部121で生成されたハッシュ値Dと復号情報Dを入力とし、データの比較を行う。

【0027】ステップ206) 比較した結果が一致すれば、検査機関がプログラムの動作を検査した後に、第三者によるプログラムが改竄されていないことが証明される。また、上記の例では、図4の構成に基づいて説明しているが、ICチップに限定されることなく、パソコン等で行うようにしてもよい。また、図6と図7の処理を別々のプロセッサで行うようにしてもよい。

【0028】また、上記の図6、図7に示す検証処理をプログラムとして構築し、ICメモリ、ディスク装置や、フロッピーディスクやCD-ROM等の可搬記憶媒体に格納しておき、本発明を実施する際にインストールすることにより、容易に本発明を実現できる。なお、本発明は、上記の例に限定されることなく、特許請求の範囲内で種々変更・応用が可能である。

【0029】

【発明の効果】上述のように、本発明によれば、プログラム提供者がプログラムを提供した後に行われた改竄を検出するのみならず、検査機関がプログラムの動作を検

査した後に行われたプログラムの改竄も検出することが可能であるため、提供されたプログラムが安全に動作することを証明することができる。

【図面の簡単な説明】

【図1】本発明の原理を説明するための図である。

【図2】本発明の原理構成図である。

【図3】本発明のシステム構成図である。

【図4】本発明のICチップの構成図である。

【図5】本発明の端末の構成図である。

【図6】本発明のプログラム提供後の改竄を検証する処理のフローチャートである。

【図7】本発明の検査機関のプログラム動作の検査後の改竄を検証する処理のフローチャートである。

【符号の説明】

1 プログラムファイル

2 入力手段

3 プログラム提供者検証手段

4 検証機関検証手段

10 ICチップ

11 メモリ

12 プロセッサ

13 入出力インタフェース

20 端末

30 証明機関サーバ

21 メモリ

22 入出力インタフェース

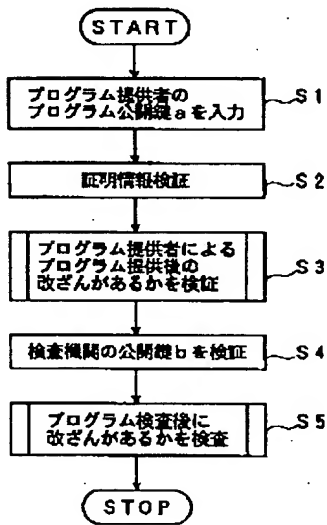
121 ハッシュ生成部

122 署名復号部

123 データ比較部

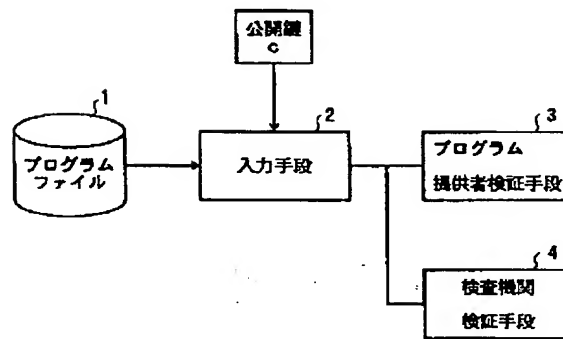
【図1】

本発明の原理を説明するための図



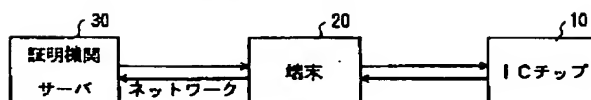
【図2】

本発明の原理構成図



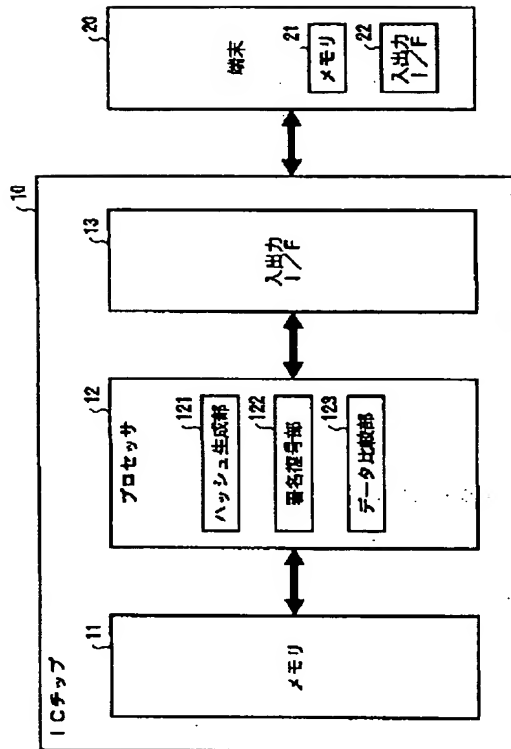
【図3】

本発明のシステム構成図



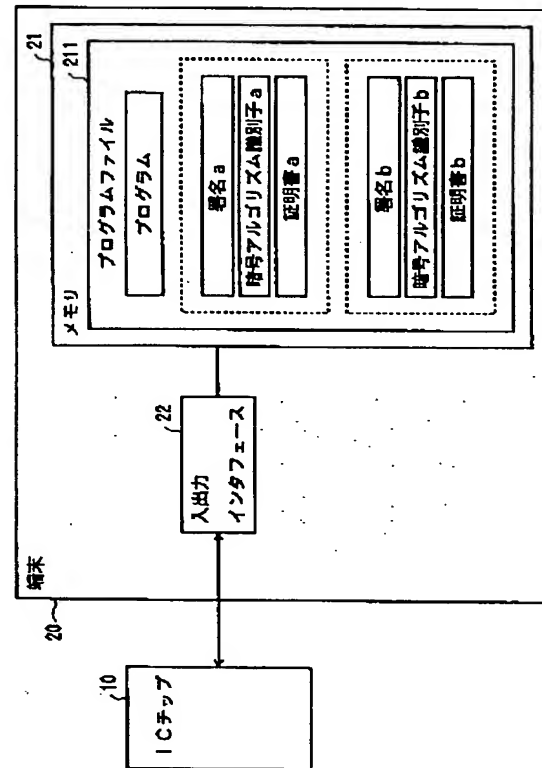
【図4】

本発明のICチップの構成図



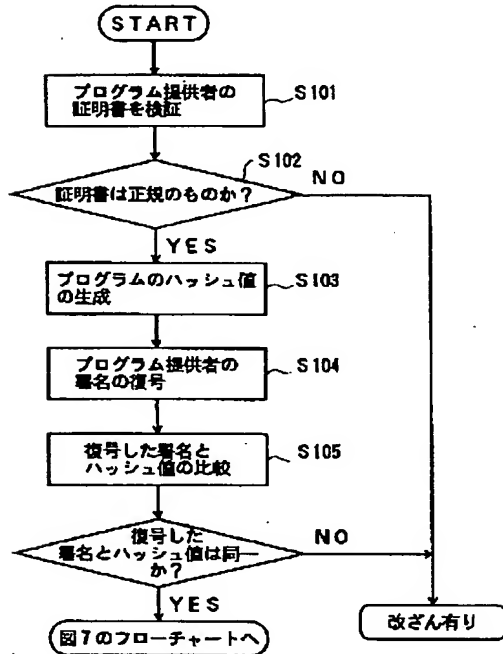
【図5】

本発明の端末の構成図



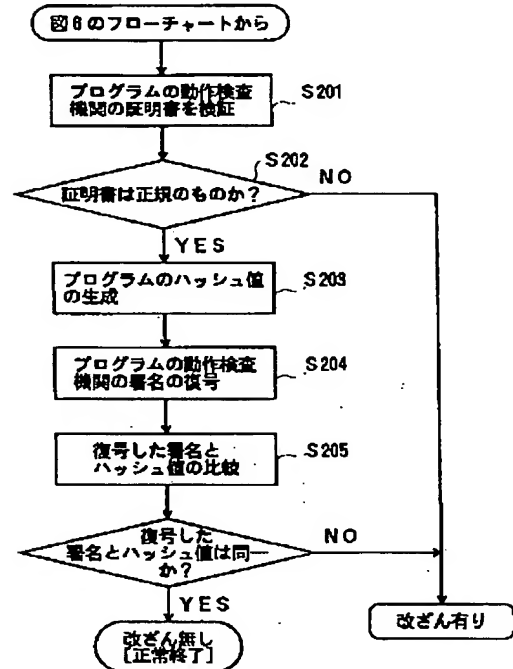
【図6】

本発明のプログラム提供後の
改ざんを検証する処理のフローチャート



【図7】

本発明の検査機関のプログラム動作の検査後の
改ざんを検証する処理のフローチャート



フロントページの続き

(72)発明者 千葉 伸浩
東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(72)発明者 細田 泰弘
東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

Fターム(参考) 5B076 FA13 FA14